Workgroup: Network Working Group
Internet-Draft:
draft-hallambaker-mesh-ceremonies
Published: 9 March 2020
Intended Status: Informational
Expires: 10 September 2020
Authors: P. M. Hallam-Baker
ThresholdSecrets.com

Mathematical Mesh 3.0 Part XIII: Mesh Ceremonies

Abstract

https://mailarchive.ietf.org/arch/browse/mathmesh/Discussion of this draft should take place on the MathMesh mailing list (mathmesh@ietf.org), which is archived at .

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 September 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction

2. Definitions

2.1. Requirements Language

2.2. Defined Terms

2.3. Related Specifications

2.4. Implementation Status

3. Device Onboarding Ceremonies

3.1. Networked Desktop to Desktop (Fingerprint Verification)

3.2. Networked Mobile to Desktop (Dynamic QR Code)

3.3. Pre-Networked Mobile to Mobile (Dynamic QR Code)

3.4. Pre-Networked Headless Device to Mobile (Static QR Code)

3.5. Mobile proxy to Desktop

4. Contact Establishment Ceremonies

4.1. In Person

4.2. Remote

4.3. Registration

4.4. Trusted Third Party Endorsement

5. Authentication Ceremonies

5.1. Second Factor Authentication

5.2. Confirmation

6. Security Considerations

7. IANA Considerations

8. Acknowledgements

9. Normative References

10. Informative References

1. Introduction

2. Definitions

This section presents the related specifications and standard, the terms that are used as terms of art within the documents and the terms used as requirements language.

2.1. Requirements Language

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in [RFC2119].

2.2. Defined Terms

2.3. Related Specifications

2.4. Implementation Status

The implementation status of the reference code base is described in the companion document [draft-hallambaker-mesh-developer].

3. Device Onboarding Ceremonies

3.1. Networked Desktop to Desktop (Fingerprint Verification)

3.2. Networked Mobile to Desktop (Dynamic QR Code)

3.3. Pre-Networked Mobile to Mobile (Dynamic QR Code)

3.4. Pre-Networked Headless Device to Mobile (Static QR Code)

3.5. Mobile proxy to Desktop

4. Contact Establishment Ceremonies

4.1. In Person

4.2. Remote

4.3. Registration

4.4. Trusted Third Party Endorsement

5. Authentication Ceremonies

5.1. Second Factor Authentication

5.2. Confirmation

6. Security Considerations

7. IANA Considerations

This document requires no IANA actions.

8. Acknowledgements

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

10. Informative References

[draft-hallambaker-mesh-developer] Hallam-Baker, P., "Mathematical Mesh: Reference Implementation", Work in Progress, Internet-Draft, draft-

hallambaker-mesh-developer-09, 23 October 2019, <https://tools.ietf.org/html/draft-hallambaker-mesh-developer-09>.